UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE INSTALLATION AND USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES ON CELLULAR TELEPHONE NUMBER 513-226-0831	**CASE NO.** 1:18MJ -282 **APPLICATION** **(UNDER SEAL)**

The United States of America, moving by and through AUSA Karl P. Kadon III, its undersigned counsel, respectfully submits under seal this *ex parte* Application for an order pursuant to 18 U.S.C §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices ("pen-trap devices") to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from the cellular telephone number **513-226-0831** (**Target Telephone**), described in Attachment A. In support of this Application, the United States asserts:

1. This is an Application, made under 18 U.S.C. § 3122(a)(1), for an order under 18 U.S.C. § 3123 authorizing the installation and use of a pen register and a trap and trace device.

2. Such an Application must include three elements: (1) "the identity of the attorney for the Government or the State law enforcement or investigative officer making the Application"; (2) "the identity of the law enforcement agency conducting the investigation"; and (3) "a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." 18 U.S.C. § 3122(b).

3. The undersigned applicant is an "attorney for the government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure.

4. The law enforcement agency conducting the investigation is the Federal Bureau of Investigation (FBI).

5. The applicant hereby certifies that the information likely to be obtained by the requested pen-trap devices is relevant to an ongoing criminal investigation being conducted by the FBI into Robert STRACKE, and other as-yet- unknown individuals, in connection with possible violations of Title 21, United States Code, Sections 841(a)(1) and 846.

6. The applicant understands that the FBI and the United States Attorney's Office are directed to comply with the limitations set forth in 18 U.S.C. § 3123(c).

7. This Court is a "court of competent jurisdiction" under 18 U.S.C. § 3122(a)(2) because it "has jurisdiction over the offense being investigated," 18 U.S.C. § 3127(2)(A)(i).

8. Other than the three elements described above, federal law does not require that an Application for an order authorizing the installation and use of a pen register and a trap and trace device specify any facts. The following additional information is provided to demonstrate that the order requested falls within this Court's authority to authorize the installation and use of a pen register or trap and trace device under 18 U.S.C. § 3123(a)(1).

9. A "pen register" is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3). A "trap and trace device" is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. § 3127(4).

THE RELEVANT FACTS

10. A Task Force comprised of investigators from the FBI, DEA, United States Postal Inspection Service (USPIS), and Cincinnati Police Department, are investigating criminal

organizations using DarkNet Marketplaces ("DNM") to distribute illicit narcotics and launder proceeds from illicit narcotics with the use of virtual currencies.1 During the course of this investigations, investigators have identified Robert STRACKE as a recipient of narcotic shipments believed to be sourced from the Darknet. STRACKE receives packages at a P.O. Box within a UPS store, located at 11711 Princeton Pike, Unit #341, Box 312, Cincinnati, Ohio 45246. According to the UPS, STRACKE has received 129 parcels to Box 312 in the last year. On April 12, 2018, UPS provided investigators with the STRACKE's telephone number as the **Target Telephone**.

11. On March 29, 2018, the investigative team conducted surveillance on 11711 Princeton Pike, Unit #341, Cincinnati, Ohio 45246 and observed STRACKE retrieve two parcels addressed, which were addressed to him. Investigators previously identified the parcels as coming from a Darkweb source and as potentially containing narcotics. Both parcels bore fictitious return names and addresses. STRACKE was observed driving a Nissan Versa, bearing Ohio registration FNG 9820, which is registered to Robert STRACKE. During the mobile surveillance, the investigative team observed STRACKE meet multiple individuals in parking lots for short periods of time, which based on your affiant's experience working drug investigations is a indicative of a drug transaction. Later on surveillance, the investigative team identified STRACKE meet Hartford Eugene PENN IV in the same manner in a parking lot. PENN is known to law enforcement as being associated with heroin distribution in the Cincinnati area. The investigative team observed that one of the parcels had been ripped open inside the STRACKE's vehicle prior to STRACKE meeting with PENN.

---

1 The term "Darknet" is a portion of routed, allocated IP space not running on any services. The term Darknet is often used interchangeably with the term "Darkweb." The Darkweb is an overlay network that can be accessed with specific software, such as the Tor web browser, which seeks to make web browsing anonymous. All Darknets require specific software installed or network configurations made to access them.

12. On April 9, 2018, the USPIS seized two parcels addressed to STRACKE mailed to 11711 Princeton Pike, Unit #341, Box 312, Cincinnati, Ohio 45246. A court authorized search warrant, signed by United States Magistrate Judge Karen L. Litkovitz, Southern District of Ohio, was obtained for these parcels. The execution of the search warrant of these parcels revealed the one package containing approximately two (2) kilograms of suspected Xanax pills while the other bag contained approximately .266 kilograms of suspected Xanax. A subsequent search of the second parcel revealed the package contained approximately 1000 suspected Xanax pills. Hamilton County Coroner's office conducted a preliminary test of the suspected Xanax, which revealed a presumptive positive test result for Alprazolam (Xanax).

13. According to UPS store surveillance on April 10, 2018, STRACKE arrived at the UPS store and retrieved another parcel. Video from the UPS store was obtained showing STRACKE taking possession of the parcel. Investigators believe this parcel was illegal narcotics purchased from a Darknet source based upon the previous seizure, surveillance, and history of parcels for STRACKE at the UPS store.

14. According to UPS store surveillance video on April 13, 2018, STRACKE came into the store and inquired to a store employee about the whereabouts of the two packages he never received, which investigators seized on April 9, 2018.

15. Based upon toll analysis of the **Target Telephone**, the **Target Telephone** has been in constant contact with (513) 903-1115. According to a law enforcement database inquiry, telephone number (513) 903-1115 is used by Hartford Eugene PENN. According to the Ohio Department of Corrections, PENN was housed in the same incarceration dormitory as STRACKE from 2014 to 2016.

16. Based on the aforementioned facts and reporting, I believe there is probable cause to show that STRACKE uses the **Target Telephone** to commit federal offenses, and that the

information requested will assist the FBI in identifying co-conspirators and additional cellular devices owned and operated by the targeted subjects.

17. In my training and experience, I have learned that providers of cellular telephone service have technical capabilities that allow them to collect and generate at least two kinds of information about the locations of the cellular telephones to which they provide service: (1) E-911 Phase II data, also known as GPS data or latitude-longitude data, and (2) cell-site data, also known as "tower/face information" or cell tower/sector records. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise that E-911 Phase II data.

18. Based on my training and experience, I know that wireless phone companies can collect E-911 Phase II data about the location of the target cell phone, including by initiating a signal to determine the location of the target cell phone on Sprint network or with such other reference points as may be reasonably available.

19. Based on my training and experience, I know that wireless phone companies can also collect cell-site data about the target cell phone.

20. Based on the aforementioned facts and reporting, I believe there is probable cause to show that Robert STRACKE is using the **Target Telephone** to commit federal narcotics

offenses and that the information requested will assist the FBI in identifying co-conspirators and additional cellular devices owned and operated by the targeted subjects.

21. The conduct being investigated involves use of the cellular telephone number described in Attachment A. To further the investigation, investigators need to obtain the dialing, routing, addressing, and signaling information associated with communications sent to or from that cellular telephone number.

22. The pen-trap devices sought by this Application will record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from the cellular telephone number described in Attachment A, including the date, time, and duration of the communication, and those items listed in Attachment B, without geographic limit.

23. In the traditional telephone context, pen registers captured the destination phone numbers of outgoing calls, while trap and trace devices captured the phone numbers of incoming calls. Similar principles apply to other kinds of wire and electronic communications, as described below.

24. A cellular telephone, or cell phone, is a mobile device that can transmit and receive both wire and electronic communications. Individuals using cellular telephones contract with cellular service providers, who maintain antenna towers covering specific geographic areas. In order to transmit or receive calls and data, a cellular telephone must send a radio signal to an antenna tower that, in turn, is connected to a cellular service provider's network. A cellular telephone connected to a cellular service provider's network can thus act much like a traditional landline telephone and a computer. This Application seeks both traditional telephone calling data (i.e., telephone numbers dialed and dialing the target device), as well as data related to the dialing, routing, addressing and signaling of electronic communications sent to and from the target device.

25. In addition to a unique telephone number, each cellular telephone has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular telephone could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEID"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), an International Mobile Subscriber Identifier ("IMSI"), a Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), or an International Mobile Station Equipment Identity ("IMEI"). When a cellular telephone connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower, and the cellular antenna or tower receives and forwards those identifiers to the core network as a matter of course. The unique identifiers—as transmitted from a cellular telephone to a cellular network—are similar to telephone numbers in that they are used by the cellular provider to identify, authenticate, and/or route the communications. They can be recorded by pen-trap devices and indicate the identity of the cellular telephone device making the communication without revealing the communication's content.

26. In addition, a list of incoming and outgoing telephone numbers is generated when a cellular telephone is used to make or receive calls, or to send or receive text messages (which may include photographs, videos, and other data). These telephone numbers can be recorded by pen-trap devices and then used to identify the parties to a communication without revealing the communication's contents.

ELECTRONIC COMMUNICATIONS

27. The Internet is a global network of computers and other devices. On the Internet, data transferred between devices is not sent as a continuous stream, but rather it is split into discrete packets. Generally, a single communication is sent as a series of data packets. When the packets reach their destination, the receiving device reassembles them into the complete communication. Each packet has two parts: a header with routing and control information, and a payload, which generally contains user data. The header contains non-content information such as the packet's source and destination Internet Protocol (IP) addresses[2], source and destination port numbers[3], transport protocol[4], flow label[5] (when IPv6 applies), and the packet's size[6]. The payload usually includes the content of the transmitted communication – for example, part of the text of an e-mail message or the data that makes up part of an electronic image.

28. Cellular phones can connect to the Internet via the cellular network. They can then be used to browse the World Wide Web, send e-mail messages, and engage in other forms of

---

[2] A numerical label that identifies the source or terminating device on an IP network transmitting an individual packet associated with a communication.

[3] Port numbers of the IP packet uniquely identify different applications or processes running on a single device (the source or destination device) and enable the devices to share a single physical connection to a network. This parameter is also used by communication providers for routing of IP packets when utilizing Network Address Translation (NAT), which is common among cellular telephone providers. The source and destination ports are numerical labels that identify the endpoints at the source and destination devices on an IP network transmitting an individual packet associated with a communication. When combined with the source and destination IP addresses, this routing information identifies the source transmitting an IP packet and the destination receiving the IP packet.

[4] The transport protocol defines the protocol used in the data portion of the IP packet. One example is the Transport Control Protocol, or TCP, which is one of the core protocols of the Internet Protocol suite. TCP provides reliable, ordered and error-checked delivery of a stream of octets between programs running on computers connected to a local area network, intranet or the public Internet.

[5] The field in the IPv6 header that is used by a source to label packets of a flow to avoid disruption during reassembly. This can facilitate such processes as streaming online video or audio feeds. The flow label can be used to indicate to routers and switches with multiple outbound paths that the listed packets should stay on the same path so that they will not be reordered.

[6] The field that defines the entire packet size, including header and data, in bytes.

electronic communications, just like desktop computers. When connecting through the cellular network, Internet communications sent and received by a cellular phone will contain some of the same unique identifiers that identify cellular voice communications, such as an ESN, MEID, MIN, SIM, IMSI, MSISDN, or IMEI. Internet communications sent to and from a cellular phone also contain the header information referenced above in each data packet, such as the source and destination IP addresses and the source and destination port numbers associated with that cellular phone at the specific time of the communication. Each of these unique identifiers can be used to identify devices that are party to a communication without revealing the communication's contents. The IP addresses and port numbers recorded in the headers of data packets also are readily available to the cellular service provider in each and every data packet (if they were not, the packets could not be routed to and from their destinations), and can easily be extracted by a pen register and trap and trace device.

29. On the Internet, IP addresses and port numbers function much like telephone numbers and area codes – often both are necessary to route a communication. Devices directly connected to the Internet are identified by a unique IP address. This number is used to route information between devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. Both the IP address of the requesting device (the source IP address) and the IP address of the receiving device (the destination IP address) are included in specific fields within the header of each packet of data sent over the Internet. Source and destination port numbers are also included in specific fields within the headers of data packets. Sometimes these port numbers identify the type of service that is connected with a communication (for example email or web-browsing), but often they identify a specific device on a private network. In either case, port numbers are used to route data packets either to a specific device or a specific process

running on a device. Thus, in both cases, port numbers are used by computers to route data packets to their final destinations.

30. The headers of data packets also contain other dialing, routing, addressing and signaling information. This data includes the transport protocol used (there are several different transport protocols that provide transport of data over networks); the flow label (which helps control the path and order of transmission of packets in certain circumstances - for example the packets that make up streaming video that must be placed in a certain order once received); and the packet size (used to identify the size of each data packet).

31. Because they are all used to facilitate the routing and transfer of data, and because they do not contain the content of communications, the United States requests that this Court order Sprint to either produce, or assist the United States in obtaining through the installation of a Pen Trap device, the IP addresses, port numbers, transport protocol, flow label and packet size of each data packet sent to and from the target device. See 18 U.S.C. §§ 3122 and 3123.

32. The United States further requests that the Court order Sprint to provide other data related to each data packet sent over the provider's network. These data fields are commonly provided by cellular telephone providers pursuant to industry standards adopted under the Communications Assistance for Law Enforcement Act (CALEA). See 47 U.S.C. § 1006. They include: the Case Identification (or Case ID), which is a unique identifier used by law enforcement and the provider to identify the case to which the data pertains; the Intercept Access Point System Identification (IAP System ID), which identifies the network equipment responsible for isolating the targeted information; the Timestamp, which identifies the date and time that the event was detected; and the Correlation Number, which provides a unique identifier for the call data that is used to correlate the communication identifying information with the communication content.

GOVERNMENT REQUESTS

33. For the reasons stated above, the United States requests that the Court enter an Order authorizing the installation and use of pen-trap devices to record, decode, and/or capture the dialing, routing, addressing, and signaling information described above for each communication to or from the cellular telephone number described in Attachment A, to include the date, time, and duration of the communication, and those items listed in Attachment B, without geographic limit. The United States does not request and does not seek to obtain the contents of any communications, as defined in 18 U.S.C. § 2510(8).

34. Based on the specific and articulable facts set forth above, pursuant to Title 18, United States Code, Sections 2703(c)(1)(B), 2703(c)(2) and 2703(d), the United States requests that Sprint be ordered to supply subscriber information (including the names and addresses of the subscriber, whether listed or unlisted, billing information, payment information, subscriber date of birth, subscriber driver license number, subscriber social security number, equipment information, shipment information, call detail records, information related to calls made via direct connect features, calls to destination search (or "reverse dumps"), and periods of telephone activation) for all numbers dialed or connections made to and from the cellular telephone number described in Attachment A captured by the pen register or trap and trace devices on the cellular telephone number described in Attachment A.

35. The United States further requests that the Court authorize the foregoing installation and use for a period of sixty (60) days from the date of the Court's Order, pursuant to 18 U.S.C. § 3123(c)(1).

36. The United States further requests, pursuant to 18 U.S.C. §§ 3123(b)(2) and 3124(a)-(b), that the Court order Sprint and any other person or entity providing wire or electronic communication service in the United States whose assistance may facilitate execution of this Order to furnish, upon service of the Order, information, facilities, and technical assistance necessary to

install the pen-trap devices, including installation and operation of the pen-trap devices unobtrusively and with minimum disruption of normal service. Any entity providing such assistance shall be reasonably compensated by the FBI, pursuant to 18 U.S.C. § 3124(c), for reasonable expenses incurred in providing facilities and assistance in furtherance of this Order.

37. If Sprint, or any other relevant provider of electronic communication service to the public, cannot comply with this Court's Order to install the pen-trap devices, the United States requests authorization to install and use its own pen register and trap and trace devices on the data network of Sprint, or any other relevant provider of electronic communication service to the public, pursuant to 18 U.S.C. § 3123(a)(3)(A).

38. The United States further requests, pursuant to 18 U.S.C. §§ 3123(b)(2) and 3124(a)-(b), that the Court order Sprint and any other person or entity providing wire or electronic communication service in the United States whose assistance may facilitate execution of this Order, to furnish immediate technical assistance to the FBI to accomplish the interception of all of the dialing, routing, addressing, and signaling information for all data packets associated with each communication to or from the target device, including the date, time and duration of the communication; and to deliver all such intercepted dialing, routing, addressing, and signaling information, securely and reliably and in a format that allows the information to be understood by the applicant. In particular, the United States requests that Sprint and any other person or entity providing wire or electronic communication service in the United States shall provide the following:

- Any requested technical documentation and necessary assistance to enable the FBI to ascertain the meaning and significance of data in the delivery; to facilitate breaking down the information into distinct identifiable fields; and to address deficiencies and preferences with formats.

- A designated technical representative(s)/engineer(s) who will coordinate efforts with and have the authority to provide the FBI technical staff the necessary information and technical assistance, including direct access to the network facilities used or controlled by or on behalf of the FBI, and any other person or entity providing wire or electronic communication service in the United States to the target device, for purposes of testing, evaluation and implementation of the technical means necessary to accomplish the authorized pen register and a trap and trace device or process.

39. The United States further requests that the Court order Sprint and any other person or entity whose assistance may facilitate execution of this Order to notify the applicant and the FBI of any changes relating to the cellular telephone number described in Attachment A, including changes to the International Mobile Subscriber Identifier ("IMSI") and/or the International Mobile Station Equipment Identity ("IMEI"), to include changes to subscriber information; and to provide prior notice to the applicant and the FBI before terminating or changing service to the cellular telephone number.

40. The United States further requests that the Court order that the FBI and the applicant have access to the information collected by the pen-trap devices as soon as practicable, twenty-four hours per day, or at such other times as may be acceptable to them, for the duration of the Order.

41. The United States further requests, pursuant to 18 U.S.C. § 3123(d)(2), that the Court order Sprint and any other person or entity whose assistance facilitates execution of this Order, and their agents and employees, not to disclose in any manner, directly or indirectly, by any action or inaction, the existence of this Application and Order, the resulting pen-trap devices, or

this investigation, unless and until authorized by this Court, except that Sprint may disclose this Order to an attorney for Sprint for the purpose of receiving legal advice.

42. The United States further requests that this Application and any resulting Order be sealed until otherwise ordered by the Court, pursuant to 18 U.S.C. § 3123(d)(1).

43. The United States further requests that the Clerk of the Court provide the United States Attorney's Office with three certified copies of this Application and Order, and provide copies of this Order to the FBI and Sprint upon request.

44. The foregoing is based on information provided to me in my official capacity by agents of the FBI.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 25th day of April, 2018.

Respectfully submitted,

BENJAMIN C. GLASSMAN
United States Attorney

s/Karl P. Kadon

KARL P. KADON (0009324)
Assistant United States Attorney
221 East Fourth Street, Suite 400
Cincinnati, Ohio 45202
Office: (513) 684-3711
Fax: (513) 684-2047